



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/611,771	06/30/2003	Juan A. Garay	Garay-10-1	2190
8933	7590	01/11/2007	EXAMINER	
DUANE MORRIS, LLP			JOHNSON, CARLTON	
IP DEPARTMENT			ART UNIT	PAPER NUMBER
30 SOUTH 17TH STREET			2136	
PHILADELPHIA, PA 19103-4196				
SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE		DELIVERY MODE	
3 MONTHS	01/11/2007		PAPER	

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

Office Action Summary	Application No.	Applicant(s)	
	10/611,771	GARAY ET AL.	
	Examiner	Art Unit	
	Carlton Johnson	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --
Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) Responsive to communication(s) filed on 30 June 2003.
- 2a) This action is FINAL. 2b) This action is non-final.
- 3) Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) Claim(s) 1-29 is/are pending in the application.
 - 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) Claim(s) _____ is/are allowed.
- 6) Claim(s) 1-29 is/are rejected.
- 7) Claim(s) _____ is/are objected to.
- 8) Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) The specification is objected to by the Examiner.
- 10) The drawing(s) filed on 30 June 2003 is/are: a) accepted or b) objected to by the Examiner.
 Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
 Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
 - a) All b) Some * c) None of:
 1. Certified copies of the priority documents have been received.
 2. Certified copies of the priority documents have been received in Application No. _____.
 3. Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- 1) Notice of References Cited (PTO-892)
- 2) Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) Information Disclosure Statement(s) (PTO/SB/08)
 Paper No(s)/Mail Date 6-30-2003.
- 4) Interview Summary (PTO-413)
 Paper No(s)/Mail Date. _____.
- 5) Notice of Informal Patent Application
- 6) Other: _____.

DETAILED ACTION

1. This action is responding to application papers filed **6-30-2003**.
2. Claims **1 - 29** are pending. Claims **1, 11, 23** are independent.

Claim Rejections - 35 USC § 112

3. Claims **4, 5, 7, 8, 18, 19** are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. The inclusion of a formula within a claim limitation renders the claim language indefinite. A formula is not searchable within the confines of current technology. Instead, a formula must be disclosed in its narrative form, which is searchable within the confines of current technology. The sequence generation formulas disclosed within the Micali prior art will be interpreted as sequence generation formulas and utilized for the generation of sequence values for this application. Applicant's specification (see Specification Paragraph [0020]) discloses the utilization of Blum integers in the generation of a sequence.

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:
 - a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been

obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

5. Claims 1 - 29 are rejected under 35 U.S.C. 102(e) as being unpatentable over ASOKAN et al. et al. (US PGPUB No. 20020049601) of Micali et al. (US Patent No. 4,944,009).

Regarding Claim 1, ASOKAN discloses a method for providing a fair exchange of user information by encoding said information with a hidden value comprising the step of: selecting said hidden value as one of a plurality of sequence values. (see ASOKAN paragraph [0010], lines 2-7; paragraph [0035], lines 1-6: fair exchange information system; paragraph [0109], lines 1-3: digital signature utilized; paragraph [0007], lines 1-4: network communications) ASOKAN does not specifically disclose difference values between adjacent ones of said sequence values are symmetrically distributed about one of said values of a known order. However, Micali discloses wherein difference values between adjacent ones of said sequence values are symmetrically distributed about one of said values of a known order. (see Micali col. 2, lines 43-47; col. 4, lines 10-13: sequence generation; col. 12, lines 45-48: Blum integers)

It would have been obvious to one of ordinary skill in the art to modify ASOKAN as taught by Micali to enable the generation of a symmetrically distributed sequence for usage in a secure information exchange procedure. One of ordinary skill in the art would have been motivated to employ the teachings of Micali in order to maintain security within a system by the usage of

longer and more secure sequences utilized within encryption procedures. (see Micali col. 4, lines 15-18: “*... To maintain the security of the system, longer sequences are best used with each encryption, and different sequences are best used in successive encryptions. ...*”)

Regarding Claim 2, ASOKAN discloses the method as recited in claim 1. (see ASOKAN paragraph [0010], lines 2-7; paragraph [0035], lines 1-6: fair exchange information system; paragraph [0109], lines 1-3: digital signature utilized; paragraph [0007], lines 1-4: network communications) ASOKAN does not specifically disclose said difference values progressively increase then decrease about said value of known order. However, Micali disclose wherein said difference values progressively increase then decrease about said value of known order. (see Micali col. 2, lines 43-47; col. 4, lines 10-13: sequence generation (i.e. progressively increasing and decreasing); col. 12, lines 45-48: Blum integers)

It would have been obvious to one of ordinary skill in the art to modify ASOKAN as taught by Micali to enable the generation of a sequence (i.e. progressively increasing and decreasing) for usage in a secure information exchange procedure. One of ordinary skill in the art would have been motivated to employ the teachings of Micali in order to maintain security within a system by the usage of longer and more secure sequences utilized within encryption procedures. (see Micali col. 4, lines 15-18)

Regarding Claim 3, ASOKAN discloses the method as recited in claim 1. (see ASOKAN paragraph [0010], lines 2-7; paragraph [0035], lines 1-6: fair exchange information system; paragraph [0109], lines 1-3: digital signature utilized; paragraph [0007], lines 1-4: network communications) ASOKAN does not specifically disclose said plurality of values are determined in accordance with a root value and a modulus value. However, Micali disclose wherein the plurality of values are determined in accordance with a root value and a modulus value. (see Micali col. 2, lines 43-47; col. 4, lines 10-13: sequence generation (i.e. root and modulus); col. 12, lines 45-48: Blum integers)

It would have been obvious to one of ordinary skill in the art to modify ASOKAN as taught by Micali to enable the generation of a sequence based on root and modulus values, and utilized in a secure information exchange procedure. One of ordinary skill in the art would have been motivated to employ the teachings of Micali in order to maintain security within a system by the usage of longer and more secure sequences utilized within encryption procedures. (see Micali col. 4, lines 15-18)

Regarding Claims 4, 18, ASOKAN discloses the method as recited in claims 1, 11. (see ASOKAN paragraph [0010], lines 2-7; paragraph [0035], lines 1-6: fair exchange information system; paragraph [0109], lines 1-3: digital signature utilized; paragraph [0007], lines 1-4: network communications) ASOKAN does not specifically disclose said sequence values are determined based on a

selected formula. However, Micali discloses wherein said sequence values are determined as:

$$\left(g^{2^{2^i}} \right)_{i=0}^K \bmod(N);$$
$$\left(g^{2^{\{(2^{K+1})-(2^{K-n})\}}} \right)_{n=1}^K \bmod(N);$$

where K is a known order;

N is a modulus value; and

g is a root value.

(see Micali col. 2, lines 43-47; col. 4, lines 10-13: sequence generation (i.e. progressively increasing and decreasing); col. 12, lines 45-48: Blum integers)

It would have been obvious to one of ordinary skill in the art to modify ASOKAN as taught by Micali to enable the usage of a sequence generation algorithm within a secure information exchange procedure. One of ordinary skill in the art would have been motivated to employ the teachings of Micali in order to maintain security within a system by the usage of longer and more secure sequences utilized within encryption procedures. (see Micali col. 4, lines 15-18)

Regarding Claim 5, ASOKAN discloses the method as recited in claim 4. (see ASOKAN paragraph [0010], lines 2-7; paragraph [0035], lines 1-6: fair exchange information system; paragraph [0109], lines 1-3: digital signature utilized; paragraph [0007], lines 1-4: network communications) ASOKAN does not

specifically disclose said sequence further comprises specific values. However, Micali discloses wherein said sequence further comprises the values: g and

$$g^{2^{2^k+1}} \bmod (N).$$

(see Micali col. 2, lines 43-47; col. 4, lines 10-13: sequence generation (i.e. progressively increasing and decreasing); col. 12, lines 45-48: Blum integers)

It would have been obvious to one of ordinary skill in the art to modify ASOKAN as taught by Micali to enable the usage of a sequence generation algorithm based on specific values within a secure information exchange procedure. One of ordinary skill in the art would have been motivated to employ the teachings of Micali in order to maintain security within a system by the usage of longer and more secure sequences utilized within encryption procedures.

(see Micali col. 4, lines 15-18)

Regarding Claim 6, ASOKAN discloses the method as recited in claim 4. (see ASOKAN paragraph [0010], lines 2-7; paragraph [0035], lines 1-6: fair exchange information system; paragraph [0109], lines 1-3: digital signature utilized; paragraph [0007], lines 1-4: network communications) ASOKAN does not specifically disclose the usage of Blum integers. However, Micali discloses wherein said modulus value is selected from the group consisting of Blum integers in the form of $N=p_1p_2$. (see Micali col. 2, lines 43-47; col. 4, lines 10-13:

sequence generation (i.e. progressively increasing and decreasing); col. 12, lines 45-48: Blum integers)

It would have been obvious to one of ordinary skill in the art to modify ASOKAN as taught by Micali to enable the generation of Blum integers for usage in a secure information exchange procedure. One of ordinary skill in the art would have been motivated to employ the teachings of Micali in order to maintain security within a system by the usage of longer and more secure sequences utilized within encryption procedures. (see Micali col. 4, lines 15-18)

Regarding Claims 7, 19, ASOKAN discloses the method as recited in claims 6, 18. (see ASOKAN paragraph [0010], lines 2-7; paragraph [0035], lines 1-6: fair exchange information system; paragraph [0109], lines 1-3: digital signature utilized; paragraph [0007], lines 1-4: network communications) ASOKAN does not specifically disclose said Blum integers are selected from a group. However, Micali discloses wherein said Blum integers are selected from the group satisfying: $p_1=2 q_1+1$; and $p_2=2 q_2+1$ wherein q_1 and q_2 are prime numbers. (see Micali col. 2, lines 43-47; col. 4, lines 10-13: sequence generation (i.e. progressively increasing and decreasing); col. 12, lines 45-48: Blum integers)

It would have been obvious to one of ordinary skill in the art to modify ASOKAN as taught by Micali to enable the usage of Blum integers for usage in a secure information exchange procedure. One of ordinary skill in the art would have been motivated to employ the teachings of Micali in order to maintain security within a system by the usage of longer and more secure sequences

utilized within encryption procedures. (see Micali col. 4, lines 15-18)

Regarding Claims 8, 20, ASOKAN discloses the method as recited in claim 7. (see ASOKAN paragraph [0010], lines 2-7; paragraph [0035], lines 1-6: fair exchange information system; paragraph [0109], lines 1-3: digital signature utilized; paragraph [0007], lines 1-4: network communications) ASOKAN does not specifically disclose a period of a sequence. However, Micali discloses wherein a period of a sequence in the form of $2^i \text{ mod } (q_1 q_2)$ is at least 2^{500} . (see Micali col. 2, lines 43-47; col. 4, lines 10-13: sequence generation (i.e. sequence period, 2^{500}); col. 12, lines 45-48: Blum integers)

It would have been obvious to one of ordinary skill in the art to modify ASOKAN as taught by Micali to enable the generation of a period of a sequence for usage in a secure information exchange procedure. One of ordinary skill in the art would have been motivated to employ the teachings of Micali in order to maintain security within a system by the usage of longer and more secure sequences utilized within encryption procedures. (see Micali col. 4, lines 15-18)

Regarding Claims 9, 21, ASOKAN discloses the method as recited in claims 1, 11, wherein said hidden value is selected as a value immediately preceding a last value of said sequence. (see ASOKAN paragraph [0010], lines 2-7; paragraph [0035], lines 1-6: fair exchange information system; paragraph [0109], lines 1-3: digital signature utilized; paragraph [0007], lines 1-4: network communications) ASOKAN does not specifically disclose said hidden value is

selected as a value immediately preceding a last value of said sequence.

However, Micali discloses wherein said hidden value is selected as a value immediately preceding a last value of said sequence. (see Micali col. 2, lines 43-47; col. 4, lines 10-13: sequence generation (i.e. hidden value immediately preceding last value); col. 12, lines 45-48: Blum integers)

It would have been obvious to one of ordinary skill in the art to modify ASOKAN as taught by Micali to enable the generation of a sequence value for usage in a secure information exchange procedure. One of ordinary skill in the art would have been motivated to employ the teachings of Micali in order to maintain security within a system by the usage of longer and more secure sequences utilized within encryption procedures. (see Micali col. 4, lines 15-18)

Regarding Claims 10, 22, ASOKAN discloses the method as recited in claims 1, 11. (see ASOKAN paragraph [0010], lines 2-7; paragraph [0035], lines 1-6: fair exchange information system; paragraph [0109], lines 1-3: digital signature utilized; paragraph [0007], lines 1-4: network communications) ASOKAN does not disclose said order value of known order is at least 80. However, Micali discloses wherein said order value of known order is at least 80. (see Micali col. 2, lines 43-47; col. 4, lines 10-13: sequence generation (i.e. order value of known order); col. 12, lines 45-48: Blum integers)

It would have been obvious to one of ordinary skill in the art to modify ASOKAN as taught by Micali to enable the generation of a sequence utilizing a value of known order for usage in a secure information exchange procedure.

One of ordinary skill in the art would have been motivated to employ the teachings of Micali in order to maintain security within a system by the usage of longer and more secure sequences utilized within encryption procedures. (see Micali col. 4, lines 15-18)

Regarding Claim 11, ASOKAN discloses a method for exchanging user information over a network comprising the steps of: transmitting over said network said user information encoded in association with a hidden value selected as one of a plurality of values distributed in a sequence wherein transmitting over said network a first set of said values and a last value in said sequence. (see ASOKAN paragraph [0010], lines 2-7; paragraph [0035], lines 1-6: fair exchange information system; paragraph [0109], lines 1-3: digital signature utilized; paragraph [0007], lines 1-4: network communications) ASOKAN does not specifically disclose a difference between adjacent ones of said values increases and decreases symmetrically about one of said values of a known order; and said values in said first set have increasing differences between adjacent ones of said values; and transmitting, individually, said remaining values in said sequence. However, Micali discloses wherein a difference between adjacent ones of said values increases and decreases symmetrically about one of said values of a known order; and said values in said first set have increasing differences between adjacent ones of said values; and transmitting, individually, said remaining values in said sequence. (see Micali col. 2, lines 43-47; col. 4,

lines 10-13: sequence generation (i.e. increasing and decreasing values); col. 12,

lines 45-48: Blum integers)

It would have been obvious to one of ordinary skill in the art to modify ASOKAN as taught by Micali to enable the generation of a sequence (i.e. sequence increasing and decreasing symmetrically, increasing differences) for usage in a secure information exchange procedure. One of ordinary skill in the art would have been motivated to employ the teachings of Micali in order to maintain security within a system by the usage of longer and more secure sequences utilized within encryption procedures. (see Micali col. 4, lines 15-18)

Regarding Claims 12, 24, ASOKAN discloses the method as recited in claims 11, 23, wherein said remaining values are transmitted in response to a received information item. (see ASOKAN paragraph [0010], lines 2-7; paragraph [0035], lines 1-6: fair exchange information system; paragraph [0109], lines 1-3: digital signature utilized; paragraph [0007], lines 1-4: network communications to transfer values)

Regarding Claims 13, 25, ASOKAN discloses the method as recited in claims 11, 23, wherein said remaining values are transmitted on a timed-basis. (see ASOKAN paragraph [0081], lines 2-5: timer (i.e. timed-basis) utilized in information transfers)

Regarding Claims 14, 15, 16, 26, ASOKAN discloses the method as recited in

claim 11, further comprising the steps of: associating a validation value with each of said plurality of values; and transmitting (i.e. concurrently, sequentially) said validation value. (see ASOKAN paragraph [0010], lines 2-7; paragraph [0035], lines 1-6: fair exchange information system; paragraph [0109], lines 1-3: digital signature utilized; paragraph [0007], lines 1-4: network communications, values transmitted)

Regarding Claims 17, 27, ASOKAN discloses the method as recited in claims 11, 23, further comprising the steps of: determining said hidden value; and decoding said user information. (see ASOKAN paragraph [0010], lines 2-7; paragraph [0035], lines 1-6: fair exchange information system (i.e. hidden values); paragraph [0109], lines 1-3: digital signature utilized; paragraph [0007], lines 1-4: network communications)

Regarding Claim 23, ASOKAN discloses a system for exchanging user information over a network comprising: a processor in communication with a memory, said processor operable to execute for: transmitting over said network said user information encoded in association with a hidden value selected; transmitting over said network a first set of said values, and a last value in said sequence; and transmitting, individually said remaining values. (see ASOKAN paragraph [0010], lines 2-7; paragraph [0035], lines 1-6: fair exchange information system; paragraph [0109], lines 1-3: digital signature utilized; paragraph [0007], lines 1-4: network communications) ASOKAN does not

specifically disclose a plurality of values distributed in a sequence wherein a difference between adjacent ones of said values increases and decreases symmetrically about one of said values of a known order, and said values in said first set have increasing differences between adjacent ones of said values. However, Micali discloses wherein a plurality of values distributed in a sequence wherein a difference between adjacent ones of said values increases and decreases symmetrically about one of said values of a known order, and said values in said first set have increasing differences between adjacent ones of said values. (see Micali col. 2, lines 43-47; col. 4, lines 10-13: sequence generation (i.e. progressively increasing and decreasing); col. 12, lines 45-48: Blum integers)

It would have been obvious to one of ordinary skill in the art to modify ASOKAN as taught by Micali to the utilization of a processor, and to enable the generation of a sequence for usage in a secure information exchange procedure. One of ordinary skill in the art would have been motivated to employ the teachings of Micali in order to maintain security within a system by the usage of longer and more secure sequences utilized within encryption procedures (see Micali col. 4, lines 15-18).

Regarding Claim 28, ASOKAN discloses the system as recited in claim 23, and disclose wherein said network operable to exchange information between said processor and said network. (see ASOKAN paragraph [0010], lines 2-7; paragraph [0035], lines 1-6: fair exchange information system; paragraph [0109],

lines 1-3: digital signature utilized; paragraph [0007], lines 1-4: network transfer of data) ASOKAN does not specifically disclose an input/device in communications with said processor. However, Micali discloses wherein further comprising: an input/output device in communication with said processor. (see Micali col. 3, lines 36-38: CPU (i.e. processor) utilized)

It would have been obvious to one of ordinary skill in the art to modify ASOKAN as taught by Micali to enable the usage of a processor in the generation of a sequence for usage in a secure information exchange procedure. One of ordinary skill in the art would have been motivated to employ the teachings of Micali in order to maintain security within a system by the usage of longer and more secure sequences utilized within encryption procedures (see Micali col. 4, lines 15-18).

Regarding Claim 29, ASOKAN discloses the system as recited in claim 23. (see ASOKAN paragraph [0010], lines 2-7; paragraph [0035], lines 1-6: fair exchange information system; paragraph [0109], lines 1-3: digital signature utilized; paragraph [0007], lines 1-4: network communications) ASOKAN does not specifically disclose the usage of memory in the generation of a sequence. However, Micali discloses wherein said code is stored in said memory. (see Micali Figure 3; col. 3, lines 30-35; col. 36-38: memory utilized)

It would have been obvious to one of ordinary skill in the art to modify ASOKAN as taught by Micali to enable the usage of memory in the generation of a sequence for usage in a secure information exchange procedure. One of

ordinary skill in the art would have been motivated to employ the teachings of Micali in order to maintain security within a system by the usage of longer and more secure sequences utilized within encryption procedures (see Micali col. 4, lines 15-18).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Carlton Johnson whose telephone number is 571-270-1032. The examiner can normally be reached Monday through Friday from 8:00AM to 5:00PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nassar Moazzami, can be reached on 571-272-4195. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

NASSER MOAZZAMI
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

C.J.

CD
1/8/07

Carlton Johnson
January 5, 2007